GSA IT

U.S. General Services Administration

MEMORANDUM FOR: Noah S. Kunin

FROM: David Shive
Acting Technology Transformation Service (TTS) Commissioner

SUBJECT: Authorizing Official Designation (AO)
TTS: Office of Products and Programs, 18F, Presidential Innovation Fellows (PIF)

DATE: 8/30/2016

Under the provisions of the CIO 2100.1,General Services Administration GSA (GSA) Information Technology (IT) Security Policy, you are hereby designated as the Designated Authorizing Official (AO) for **TTS, for all Federal Information Processing Standard (FIPS) 199 Low and Moderate Impact systems**. As an AO, you will identify the level of acceptable risk for an IT system or application and determine whether the acceptable level of risk has been obtained.

As AO you may grant or decline Authorization to Operate (ATO) in accordance with the Assessment and Authorization (A&A) guidance documented in the latest version of the Managing Enterprise Risk: Security Assessment and Authorization Planning and Risk Assessment [CA, PL & RA] [CIO Security 06-30].

The following pages contain specific responsibilities of the AO as detailed in CIO 2100.1. In carrying out your responsibilities, you should coordinate with the Program Manager of each IT resource under your responsibility. You should direct any questions regarding your duties to the GSA Administrator. If you have any questions regarding this Designation Letter, please contact the OCISO ISP Division at isp-federal-staff@gsa.gov.

GSA IT Security Policies, Guides, Points of Contact, and Forms, etc., are available on the GSA CIO website: https://insite.gsa.gov/portal/category/534722

This designation is valid until revoked by proper authorities and or superseded by another authorization.

X (b) (6)

Authorizing Official

Note: Maintain with permanent A&A file.

AO Responsibilities:

- Ensuring adherence to GSA's IT Security Policy
- Reviewing and approving security safeguards of information systems and issuing accreditation statements for each information system under their jurisdiction based on the acceptability of the security safeguards of the system (risk-management approach).
- Ensuring that an Interim Authorization to Operate (IATO) is granted, only if the necessary security enhancements to bring the system to the acceptable level of risk have been identified and a formal Plan of Action and Milestones (POA&M) has been developed. Information systems with an expiring ATO may perform a one-time extension of the current authorization for a period not to exceed one year (365 days) from the date of ATO expiry to allow development of near real-time continuous monitoring capabilities to support ongoing authorization.
- Ensuring that GSA systems that are planned to be decommissioned may request a one-time ATO extension for a period not to exceed one year (365 days) from the date of the ATO expiry.
- Ensuring that GSA information systems that are planned to be consolidated into another system or transitioned into a cloud environment may request an ATO extension, for a period not to exceed one year (365 days), to allow the information system to receive an ATO as part of the consolidated information system or its new cloud environment of operation. The scope of consolidation and/or the change in the system environment shall be approved by Office of the Chief Information Security Officer (OCISO) prior to submitting the ATO extension request for the system.
- Ensuring that GSA information systems that have undergone a full security assessment of all NIST SP 800-53 controls at the appropriate FIPS 199 impact level as part of a three-year re-authorization, and have outstanding high and critical vulnerabilities identified as part of security assessment, may request a limited ATO extension for a period not to exceed 30 days from the date of the ATO expiry to allow mitigation of the high and critical vulnerabilities.
- Ensure that new GSA information systems pursuing an agile development methodology and residing on infrastructures that have a GSA ATO concurred by the OCISO or a FedRAMP ATO may request a limited ATO for the pilot period of the project not to exceed one year (365 days). The limited ATO will be based on a lightweight security assessment and authorization (A&A) process; however, the period of the limited ATO should be used to conduct a full A&A resulting in a new three-year ATO.
- Ensuring that under any and all circumstances, in which an ATO is issued for less than three years, the GSA system continues to perform monthly Operating System scans (with Root/Administrative privileges), Database scans (DBA privileges) and Web Application scans (authenticated user privileges). All vulnerabilities identified from the scans shall be resolved; tracked in the systems' POA&M; and submitted to the GSA OCISO.
- Providing support to the Information System Security Manager (ISSM), of record appointed by the CISO.
- Providing support to the Information Systems Security Officer (ISSO) of record, appointed by the CISO for each information system.
- Ensuring Information Assurance (IA) is included in management planning, programming budgets, and the IT Capital Planning process.
- Requiring written notification of point(s) of contacts within other Federal agencies or outside organizations that manage GSA systems.
- Ensuring that IT systems that handle privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes GSA Order CIO 1878.1, GSA Order CIO 1878.2, and NIST SP 800-53
- Reviewing and approving Privacy Impact Assessments (PIAs) for their organizations.
- Supporting the security measures and goals described in Chapter 3(i) (Performance Measures) of this policy.
- Ensuring all incidents involving data breaches which could result in identity theft are coordinated through the GSA OCIO Office of the Chief Information Security Officer (OCISO) and the GSA Management Incident Response Team (MIRT) using the GSA breach notification plan per OMB

Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, IT Security Procedural Guide: Incident Response (IR), CIO-IT Security-01-02 and GSA Order, CIO 9297.2B, GSA Information Breach Notification Policy.

- Ensuring contingency and continuity of support plans are developed and tested annually in accordance with OMB Circular No. A-130, NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and IT Security Procedural Guide: Contingency Planning, OCIO-IT Security-06-29.
- Implementing detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in GSA business operations.
- Establishing physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.
- Ensuring GSA Office of Inspector General (OIG) has access to systems as described in CIO 2100.1 GSA Information Technology Security Policy.
- Establishing appropriate system/organization unique rules of behavior for systems under their authority.
- Ensuring that IT systems that handle payment card data meet the security requirements of the in Payment Card Industry Data Security Standard